International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 – No. 11, February 2018 – www.ijais.org

Proficient and Reliable Anonymous Routing Protocol (RARP) in Mobile Ad Hoc Network Environment using Digital Signatures

K. O. Boateng
KNUST
College of Engineering
Dept. of Computer Eng.

William Asiedu
University of Edu, Winneba
College of Techn Education
Dept. of Info. Techn Education

ABSTRACT

A lot of attention has been drawn to ensuring a secure communication in an ad hoc network environment. It is important to anonymously send and receive sensitive data from secure sources. Digital signature is one of the powerful ways of ensuring integrity, privacy, confidentiality and nonrepudiation in terms of signing messages. A technique from RSA is employed to propose a new digital signature to be used in wireless networks. This concept also ensures both source and location anonymity. Adversaries will find it difficult to identify the source of a message and exactly where the message is being sent to. With regard to a zone, it will not be possible to identify who sends a message and also who receives it within the group in the zone. It is believed that the signature is light weight and can easily be generated by any of the nodes in the zone. In the context of using the scheme without wireless network, individual uses alternative steps for signing sensitive documents by classifying data according to their sensitivity such as classified, secret or top secret data. This scheme also generates group signatures with multiple public keys which correspond to the group members instead of one public key for each group which is implemented in most other group signature schemes.

Keywords

Digital Signature, Anonymity, Privacy, Confidentiality, Adversaries, RSA, Communication, Location.

1. INTRODUCTION

The communication system is continuously being reformed due to the emergence of new technologies, hence enabled the technology in mobile device is a bit challenge. In ad hoc networks all the nodes cooperate with each other by forwarding packets for each other to allow them to communicate beyond their transmission range. An ad hoc network does not require any infrastructure or centralized administration like access point or base stations to set up as needed. It consists of a set of mobile nodes that are connected by wireless links. The network topology in such a network may keep changing randomly. Routing protocols that find a path to be followed by data packets from a source node to a destination node used in traditional networks cannot be directly applied in ad hoc wireless networks due to their highly dynamic topology. Military exercises, disaster relief, and mining site operations, for example, may benefit from ad hoc networks. Secure and reliable communication is very important in various applications[1]. But a wireless communication system faces challenges which include flow control over wireless multi-hop communication, error control over wireless links, deriving and maintaining routing network topology information, deriving accurate routing information, a mechanism to handle router mobility, shared channel access by multiple users, the processing capability of terminals and size, and power requirements.

Communication privacy in MANET is of great concern to a large variety of application domains, and therefore techniques to achieve high privacy assurance are needed[2]. An important privacy requirement for MANET is represented by the anonymity of the communication parties. With regard to wireless networks, many scenarios have shown that anonymity is critical. For example, the relationship of the identities of WLAN or cellular users and their locations need to be hidden from third parties [2]3], locations of the source in scenario networks should not be traced by malicious nodes[4], and active paths and network topology need to be protected in MANETs; otherwise, nodes could be traced[5].

This paper considers what it takes to provide secure communication in hostile and suspicious MANETs. It has constructed a framework for anonymous routing in MANETs which demonstrates the feasibility of simultaneously obtaining both strong privacy and strong security properties using group signatures. By privacy properties, we mean node anonymity and resistance to tracking, whereas security properties include node/origin authentication and location integrity [1]. In group signature, each group member can sign documents on behalf of the whole group. The receiver of a signed document can verify the signature to ensure that the document is signed by a group member [4]. However, no one except the group manager can recover the exact identity of the signer. The ID-based encryption scheme adapts the concepts of bilinear pairing to generate private and public keys for each user in the network [4][5]. The RARP consists of two main parts: the first one is initial setup and then, the anonymous routing phase. In the first stage, all member nodes obtain a group public key and ID-based private key from the group manager. In the second phase, anonymous routing is achieved by anonymously establishing session keys with neighbors who anonymously discover routes and anonymously forward data.

The following assumptions are considered in the environment of this research.

[LOCATION] each MANET node can securely and reliably obtain its present position most likely through GPS.

[TIME] all MANET nodes maintain loosely synchronized clocks

[RANGE] all nodes have uniform transmission range.

[MOBILITY] at least K nodes move at roughly the same time.

The remainder of this paper is organized as follows: Section 2 discusses related works or literature. It discusses a number of studies done by other researchers in anonymous routing. A detailed discussion of group signature is done in Section 3. In Section 4, the various security analyses on the proposed protocol are presented. Section 5 gives a report on the performance evaluation with other protocol and finally, a conclusion is presented in Section 6.

2. RELATED WORKS

Studies done in anonymous communication are mostly based on onion routing protocol, where packets are wrapped in a series of encrypted layers to form what is termed as onion. The intermediate nodes encrypt the data and forward it to their neighbors. The anonymous On-Demand Routing protocol Kong and Hong [12] propose uses one time private/public key pairs to achieve anonymity and unlinkability. However, their protocol fails to assure content unobservability. Yang et al. [21] enhance this protocol to achieve substantially lesser computation and communication complexities at the cost of reducing privacy guarantee. The work of Yang et al. only provides routing privacy and source anonymity. They also fail to deal with the destination anonymity.

Seys and Preneel [5] also propose a protocol which uses one-time public/private key pairs just like ANDOR but their key pairs follow only route anonymity discovery and data forwarding. Another scheme proposed by Lui et al. [14] in hierarchical anonymous routing provides inter-group and intra-group anonymity in MANET. This scheme preserves routing anonymity and controls the computational overhead by use of hierarchical routing scheme. On-Demand Lightweight Anonymous Routing (OLAR) scheme by Qin et al. [21] provides a secret sharing scheme based on the properties of polynomial interpolation mechanism to achieve anonymous message transfer without per-hop encryptions and decryptions. The cost is less than traditional cryptographic operations since the scheme tasks a forwarder (intermediate nodes) to perform simple addition and multiplications.

The Efficient Strong Anonymous Routing (MASR) Protocol scheme by Pan and Li [16] suffers from high routing overhead and computational cost since they also use onion routing scheme to achieve anonymity.

Li et al. in an efficient anonymous routing protocol for mobile ad hoc networks scheme detect malicious nodes and isolate them from the network. They also adapt onion routing to achieve anonymity but here the nodes (forwarders) encrypt the entire message with trust key and says HELLO to its ancestor within expiration time. Furthermore, Nezhad et al. propose a V-routing based on proactive routing protocol which hides the location and identity of the communicating parties but fails to provide a strong security for the data. Defrawy et al. [17], on the other hand, propose an anonymous routing protocol with multiple routes (ARMR) and Choi et al. [18] also propose an anonymous and secure reporting (ASR) which use multiple routes for communication and one-time public/private key pairs to achieve anonymity and unlinkability. ASR is designed to achieve stronger location privacy and ARMR uses bloom filter to establish more routes.

[15] The proposed Anonymous On-Demand Routing (MASK) scheme also uses onion but needs to reveal the destination ID for on-demand route discovery. That is, the tracer knows which node is the destination, yet the tracer does not know where the destination is. Sy et al. [13] use On-Demand Anonymous Routing (ODAR) in their scheme. They also use public key cryptosystem for anonymous routing.

3. GROUP SIGNATURES

Traditional public key signatures with additional privacy features can be viewed as group signature [20]. In a typical group signature scheme, any member in the group can sign a message to produce a group signature [8]. Anyone with constant –length public key can verify the group signature. A valid group signature implies that the signer is a bona fide group member. Moreover, when given any two valid group signatures, it is computationally infeasible to decide whether they are generated by the same or different group members. Only the group manager can force a signature and actually identify the signer should a dispute arise. Based on this idea, it can be boldly said that group signature is best fit for foreseen MANET settings. Multiple group signatures are not linkable, therefore, mobile nodes can periodically sign their current location information without any fear of being tracked. In the same way, anyone can verify a group signature and be assured that the signer is a legitimate MANET node. A group signature scheme has the following basic participants [19][20]:

Group Manager (GM): This entity is responsible for administering the group: initializing the group and handling members who join and leave (revocation). It is also responsible for de-anonymizing a signature in case of a dispute. Sometimes the task of adding new members is given to a separate Revocation Manager.

Group members: user/entities that represent the current set of authorized signers. In this case, a signer/member is a legitimate MANET node. Each member must have a unique private key that allows it to sign on behalf of the group.

Outsiders: any other user/entity external to the group. Outsiders are assumed to possess the group public key and are thus able to verify group signature.

Each group member must have a secret long-term identity which is tied to the group and to the member's unique private key. However, only the GM knows the relationship between the group members and their long term identities.

A group signature scheme consists of the following components[11][12]:

- ✓ SETUP: a probabilistic polynomial time algorithm, run by the GM that outputs cryptographic specification for the group, including the group manager's public and private keys.
- ✓ JOIN: a protocol between the GM and a new user that results in the user becoming a group member. The output of this protocol includes some private output for the user and a membership key.
- ✓ SIGN: an algorithm executed by any group member on the output of a message, a group public key and a member's private input outputs a group signature.
- ✓ VERIFY: an algorithm run by anyone, which on input of a message, a group public key and a group signature, output a binary flag that indicates the validity of the said group signature.

- ✓ OPEN: an algorithm run by the GM on the input of a message a group signature, a group public key and a group manager's secret key, verifies whether the group signature is valid and returns the signer's group identity and evidence that allows anyone to verify the group identity of the actual signer. It may also return no answer which is assumed to mean that the group manager is the signer.
- ✓ REVOKE: an algorithm performed by the GM to remove (revoke) a user from the group. It results in a new group public key and /or a set of auxiliary information aimed at either signers or verifiers.

Some recently proposed group signature schemes require less than 10 exponentiations to sign [25]. Though they are still appreciably more expensive than regular signatures, group signatures are rapidly becoming practical. This scheme is based on the RSA method to generate a group digital signature. The entire network will be grouped in to zones. Each zone will generate its own digital signature based on the proposed scheme. The table below shows related groups in the entire network.

Table1: Zone context information sample table

Group type	**Users**	**Private keys**	**Public keys**	**Digital representation of context**
ZX_1	ZX_1U_1, ZX_1U_2, ZX_1U_3	DC_{11}, DC_{12}, DC_{13}	EC_{11}, EC_{12}, EC_{13}	DG_1
ZX_2	ZX_2U_1, ZX_2U_2	DC_{21}, DC_{22}	EC_{21}, EC_{22}	DG_2
.	.	.	.	.
.	.	.	.	.
ZXn	ZX_nU_1, ZX_nU_2,.., ZX_nU_m	DCn$_1$, DC_{n2},…, DC_{nk}	EC_{n1}, EC_{n2},.., EC_{ik}	DG_n

For example if we assume that M denotes any message in each group or zone, e for public keys and d for private keys. Hence: $Z_n = ZX_nM_n^{dk}$. To generate a digital signature, the following steps are followed:

a. Choose the zone group type and let it CX_1

b. Select the proper key prime numbers assigned to CX_1 and let them p_1 and q_1. Then the member of that generates n_1 as follows:
$n_1 = p_1 * q_1$
then they must calculate $y(n_1)$ as follows:
$y = (p_{1-1})(q_{1-1})$

c. Generate the group digital signatures for each element in the set of authenticated users using the private key for each member as follows (which constitute the digital signatures group set SG):

$$C_1 = M_1^{d1} mod\, n\,, C_2 = M_1^{d2} mod\, n\; and\; C_3 = M_1^{d3} mod\, n$$

Therefore the group signature of the message is:
SG = {C1, C2, C3}

d. Generate the signatures of digital representation of context type DG1 as explained below:

$$C_1 = DG_1^{d1} mod\, n\,, C_2 = DG_1^{d2} mod\, n\; and\; C_3 = DG_1^{d3} mod\, n$$

The above formulas represent the group signature of the message context DG_1 and can be represented as follows:
SG'= { C1', C2',C3'} so, the resultant group signature is a combination of both message group signatures and the group context signatures.

e. These signatures sets are sent to the signature manager with the context type of the group. So the group signature appears as a block in the following form: SGF=[SG, SG',CZ_1]. The signature manager sends this block to the receiver.

f. At the recipient's end, the receiver extracts the context type CX_1 from Table 1 to find the corresponding users of this type in order to obtain their public keys. The receiver can examine each signature element and decrypt it by using the following procedures:

$$M_1 = C_1^{e1}, M_1 = C_2^{e2}, M_1 = C_3^{e3}$$

$$DG_1 = C_1^{e1}, DG_1 = C_2^{e2}, DG_1 = C_3^{e3}$$

g. If the message M_1 matches the corresponding message and DG_1 is the same as the original DG_1 value stored in table1, then the group signature (SGF) is authenticated, but if one or more signatures do not match the stored DG_1, then the group signature is rejected and considered as unauthenticated. For example, if one user from another context generates its own signature and considers it to belong to context ZX_1, this signature will not match the corresponding DG corresponding to ZX_1, hence the group signature is rejected. On the other hand, this user can generate an authenticated signature inside his/her context type. Note that Table 1 must be maintained at a sender's side and a receiver's side in a secure form.

4. PRIVACY AND SECURITY ANALYSIS

An analysis of the privacy and security related goals achieved by RARP protocol is done and compared with the MASK.

4.1 Privacy Analysis

The main difference between RARP protocol and MASK is that RARP relies on established keys between per-hop nodes to achieve privacy and security, while MASK protocol uses one-time pairing-based keys for preserving privacy. In MASK protocol, one-time pairing-based keys are generated by a trusted manager in advance whereas per-hop protection provides complete anonymity in terms of unlinkability and unobservability. However, the identity of the node information is well protected in this protocol by use of random route pseudonymity, but MASK leaks identity information of the recipient during route discovery process

4.1.1 Anonymity

A concept of pseudonymity where pseudonyms are assigned as IDs for all mobile nodes is employed. The anonymity is accomplished through group signature by using pseudonyms without revealing the user's actual identity. In route discovery process, a session key is used to establish the route while group signature is used to establish session keys anonymously between per-hop nodes. Since the group signature is secure, it therefore satisfies anonymity requirements.

4.1.2 Unlinkability

In this study, session key encryption function from cryptographic ensures that the cryptanalysts cannot understand the relation between the input and the output. That is a source node is not linkable to any sender's pseudonym and any transmission is not linkable to a particular sender's pseudonym. The same thing applies to the destination node. More specifically in communication, for a sender and a receiver, it is not possible to trace who communicates with whom even though it may be possible to find out who the sender or the receiver is. It is very difficult for the cryptanalysis to discover the relation between the sender and recipient of a particular pseudonym. In fact, in multicast a sender's and a recipient's pseudonyms are unlinkable.

4.1.3 Unobservability

RARP protocol also protects nodes from being exposed. Thus mobile nodes involved in a routing procedure are anonymous to the other nodes. A sender chooses the nonce randomly and uses it only once. There is no relation among pseudonyms which are computed from nonces. This means that could-be sender or could-be recipient's transmission is not noticeable. This is because; only the mobile nodes with valid session keys can identify the respective pseudonyms and obtain the plain text by decrypting the matching cipher text.[19] Likewise, a mobile node creates the session key anonymously with its previous or next mobile node and no one can recognize the real individualities of the in-between nodes on en-route.

4.2 Security Analysis

In this section RARP provides security issues and countermeasures through anonymity during per-hop authentication, route discovery and data forwarding.

4.2.1 Timing and Data Analysis

It can be assumed that an adversary can observe a data transmission and monitor the flow of traffic based on timing information recorded during a transmission. The adversary can use temporary dependency between transmissions to trace a victim's messages' forwarding path based on definition by [2] which states that X and Y are sets of explicit attributes of a temporal relation schema, R. A temporal functional dependency, denotes X →Y, exists on R if, for all instances r of R, all snapshots of r satisfy the functional dependency

X →Y.

But in EAR protocol, intermediate (forwarding) nodes use random pseudonym while forwarding data packets and to prevent timing and data analysis, the intermediate nodes forward fake packets associated with pseudonyms in addition to the original data packets. The pseudonyms related to the original data packets are dissimilar from the pseudonyms associated with fake packets.

An adversary will find it very difficult for data analysis and timing when original and fake packets are mixed together especially when traffic is high. However, when traffic is low, a lot of fake packets have to be generated to confuse the adversary.

4.2.2 Node Compromise

Due to the nature of an ad hoc network, an attacker can secretly penetrate into the network and compromise individual nodes or even attack a node. When a node is compromised, the attacker can extract private signing keys, ID-based encryption keys and established keys with neighboring nodes [11]. In RARP protocol, per-hop authentication and onion routing scheme are employed during the route discovery and packet forwarding stage. Therefore, the private signing key and ID-based encryption key when compromised, the adversary cannot extract location, routes and real identities of the sender/recipient node or cannot get any useful privacy information. This is because the privacy information obtained by the adversary will contain a one-hop neighbor.

4.2.3 Collusion Attack

Since RARP protocol is based on per–hop authentication and key establishment by use of group signature, there is no way in which two or more signatures will be the same. RARP supports both sender and recipient unobservability. Relationship observability means that it is not noticeable whether anything is sent from a set of could-be senders to could-be recipients.

4.2.4 Sybil Attack:

In this attack [4], a single node attempts to adopt multiple identities using only one physical device. The attacker can obtain additional identities either by making use of fake identities or by impersonating other nodes. The mobile ad hoc network is prone to this attack due to its autonomous nature that is, nodes move freely about. RARP protocol allows nodes to join a centralized key manager (Group Manager). The group manager generates group signature signing key and ID-based private key for all nodes, therefore, it is not possible for an attacker to obtain the real identities of nodes except when they are compromised.

5. PERFORMANCE EVALUATIONS

The protocol to provide the computational cost was simulated and the performance and effectiveness were analyzed against the existing scheme.

5.1 Simulation Setup

The EAR protocol in an ad hoc network is implemented in ns2 simulator version 2.32 with network size 700m x700m which consists of 100 mobile nodes. The blue color denotes the group manager and the red color denotes an adversary. The mobile nodes move in the field according to the random waypoint model [12] and their average speed ranges from 0 to 10m/s. The radio range is 250m and a bidirectional constant bit rate traffic is generated. The proposed protocol implements the group signature with a security strength of 1024-bit RSA algorithm. SHA-1 is used as the hash function to encrypt packets during the route discovery and data forwarding stage.

Table 2: Computation Cost

Techniques	**values**
Group Signature Generation (GSG)	60ms
Group Signature Verification (GSV)	65ms
SHA-1	10ms

This protocol is evaluated in terms of

1. Packet delivery ratio – data packets successfully delivered to the destination generated by the source.
2. Packet latency – time taken to deliver a packet from source to destination
3. Routing overhead - total number of control packets transmitted for each packet delivery
4. Throughput – the average number of data packets transmitted per unit of time.

5.2 Simulation results

The performance is analyzed while the parameter of packets delivery ratio, routing packet overhead, packet delivery latency and throughput are observed. Figure 1 shows the performance of RARP protocol and MASK at different speeds of a node with a traffic load of 4 packets/second. As the figure indicates, RARP has a better packet delivery ratio than MASK. The packet delivery ratio increases as the node speed also increases in both protocols. MASK packet delivery ratio is around 95% while RARP is about 96% when there is no mobility.

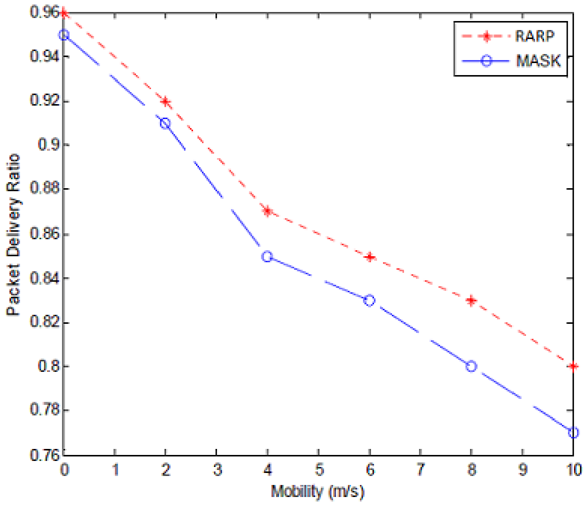

Fig. 1 Packet Delivery Ratio vs Mobility

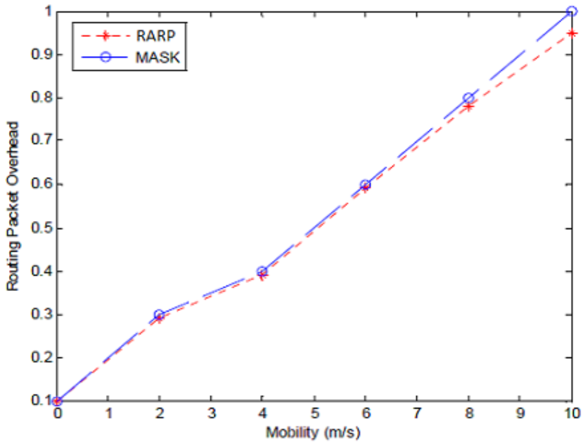

Fig 2 Routing Packet Overhead vs Mobility

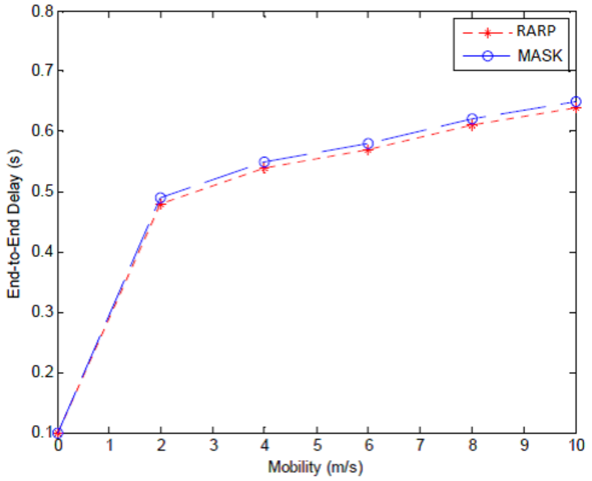

Fig 3 End-to-End Delay vs Mobility

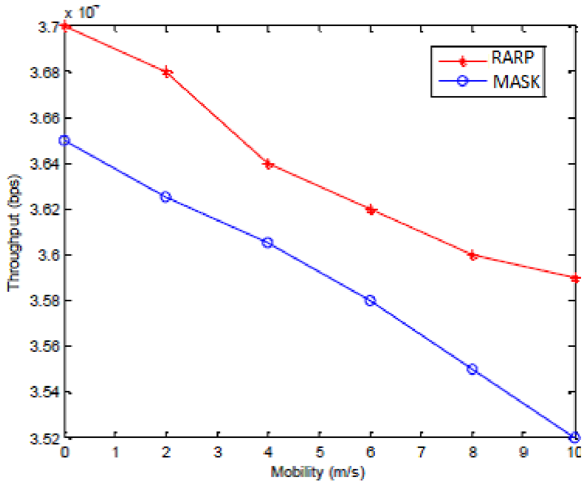

Fig 4 Throughput vs Mobility

In Figure 2, the routing cost for delivering a unit of data packet shows much improvement in MASK when compared to RARP. But nevertheless, there is not much deviation when the nodes are stable. In Figure 3, both protocols show almost the same end-to-end delay although the RARP shows a little better. In Figure 4, the performance of the throughput is highly better in RARP than MASK, but both decrease as their speed increase.

6. CONCLUSION AND FUTURE WORK

This paper proposes RARP, an anonymous routing protocol that adopts group signature and ID based encryption. It exposes adversaries and achieves untraceable and unlinkability in packet delivery. Further research can be done in the area of computational cost. Signature computation is very high and drains a lot of energy from the mobile device since most mobile devices are battery powered. It is believed that when the signature length is reduced, it will significantly improve on its performance.

7. REFERENCES

[1] Menezes, P. Van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997

[2] Abusalah, L, Khokhar, A. and Guizani, M, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE

Communications Surveys & Tutorials, 2008, 10, (4), pp. 78-93.

[3] Y. Zhang, W. Liu and W. Lou. Anonymous communications in mobile ad hoc networks. In Proceedings of the 24th international conference of the IEEE communications society (INFOCOM 2005). IEEE, 2005.

[4] D. Boneh, X. Boyen and H Shacham. Short Group Signatures. In proc. Advances in cryptology, lecture notes in computer science, springer-verlag, vol.3152, pp.41-55, aug. 2004.

[5] S. Seys, and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc networks," in proc. of the international conference on advanced information networking and applications, Vienna 2006, pp. 133-137

[6] Miranda H. and Rodrigues H. 2002. Preventing Selfishness in Open Mobile Ad Hoc Networks, In Proceedings of CaberNet Radicals Workshop.

[7] Kannhavong B. , Nemoto Y. and Kato N. , "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91, 2007.

[8] Andel T. R. and Yasinsac A. , "Surveying Security Analysis Techniques in MANET Routing Protocols", IEEE Communications Surveys and Tutorials, vol. 9, no. 4, pp. 70-84, 2007.

[9] Boneh D. and Frankliny M. 2003. Identity-Based Encryption from the Weil Pairing", In Proceedings of Advances in Cryptology.

[10] Han, S, Wang, J. and Liu, W. 2004. An Efficient Identity-Based Group Signature Scheme over Elliptic Curves", Springer LNCS.

[11] Reed, M, G, Syverson, P, F. and Goldschlag, D, M. "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482-494, 1998.

[12] Kong, J. and Hong, H. 2003. ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, In Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing.

[13] Sy, D, Chen, R. and Bao, L. 2006. ODAR: On-Demand Anonymous Routing in Ad Hoc Networks, In Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems.

[14] Liu, J, Hong, X, Kongt, J, Zheng, Q. and Bradford, P, G. 2006. A. Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks", In Proceedings of the International Conference on Military Communication.

[15] Zhang, Y, Liu, W, Lou, W. and Fang, Y, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE Transactions On Wireless Communications, vol. 5, no. 9, pp. 2376 –2385, 2006.

[16] Pan, J. and Li, J. 2009. MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Networks, In Proceedings of the International Conference on Management and Service Science.

[17] Defrawy, K,E. and Tsudik, G, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transaction on Mobile Computing, vol. 10, no. 9, pp. 1345 –1358, 2011.

[18] Heesook C. , William E. , Jaesheungn S. , Patrick D. M. and Thomas F. L. P. , "ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks", Wireless Networks, pp. 525-539, 2009.

[19] Z. Wan, K. Kui, and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Transaction on Wireless Communications, vol. 11, no. 5, pp. 1922-1932, 2012.

[20] Schnorr, C, "Efficient Signature Generation from Smart Card", Journal of Cryptography, Springer –Verlag, vol. 4, no. 3, pp. 239-252, 1991.

[21] Q. Yang, H. Dijiang, and K. Vinayak, "OLAR: On-demand Lightweight Anonymous Routing in MANETs," in Proc. 4th International Conference on Mobile Computing and Ubiquitous Networking, Tokyo, 2008, pp. 72-79.